IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	B.M. Jakobsson et al.
Case:	EMC-06-463
Serial No.:	10/631,989
Filing Date:	July 31, 2003
Group:	2137
Examiner:	Tamara Teslovich

Title: Method and Apparatus for Graph-Based Partition
of Cryptographic Functionality

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter "Appellants") hereby appeal the rejection dated August 4, 2009, of claims 1-30 of the above-identified application.

The fee previously paid with the prior Appeal Brief filed on April 13, 2009, should be applied to the present appeal. Please charge any fees which may be required to Deposit Account No. 50-0762.

REAL PARTY IN INTEREST

The real party in interest is RSA Security Inc., the assignee of record, which is a subsidiary of EMC Corporation.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

The present application was filed on July 31, 2003 with claims 1-30, all of which remain pending. Claims 1 and 28-30 are the independent claims.

Claims 1-30 are rejected under 35 U.S.C. §102(b). Claims 1-30 are appealed.

STATUS OF AMENDMENTS

There have no amendments filed subsequent to the Office Action dated August 4, 2009 (hereinafter "the Office Action"). Although the Office Action states that a "request for continued examination under 37 CFR 1.114 was filed in this application after appeal," such is not the case. Rather, the Office Action represented a reopening of prosecution by the Examiner responsive to the Appeal Brief filed on April 13, 2009, in accordance with MPEP 1207.04.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The method comprising the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level. The transmitted information includes the first seed but not the second seed.

As described in the specification at, for example, page 6, lines 6-25, an illustrative embodiment includes a method (e.g., 300 in FIG. 3) for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device (e.g., 102D in FIG. 1) to at least one recipient device (e.g., 104R in FIG. 1). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page 6, lines 19-21, the method comprises the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 28 is directed to an apparatus comprising a processing device comprising a processor coupled to a memory. The processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The processing device is configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 22, to page 6, line 5, an apparatus (e.g., 102D in FIG. 1) comprises a processing device comprising a processor (e.g., 200 in FIG. 2) coupled to a memory (e.g., 202 in FIG. 2). As described in the specification at, for example, page 4, lines 24-26, and page 6, lines 6-25, the processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device (e.g., 102D in FIG. 1), to at least one recipient device (e.g., 104R in FIG. 1). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page 6, lines 19-21, the processing device is configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 29 is directed to an apparatus comprising a processing device comprising a processor coupled to a memory. The processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes, and a given set of the nodes is associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality. The processing device is operative to receive from the delegating device information representative of one or more of the nodes, and the processing device is configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the received information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 22, to page 6, line 5, an apparatus (e.g., 102R in FIG. 1) comprises a processing device comprising a processor (e.g., 200 in FIG. 2) coupled to a memory (e.g., 202 in FIG. 2). As described in the specification at, for example, page 6, lines 6-25, the processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device (e.g., 102R), from at least one delegating device (e.g., 102D). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14, and a given set of the nodes is associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 19-25, with reference to step 302 in FIG. 3, the processing device is operative to receive from the delegating device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the processing device is configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 30 is directed to a machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The one or more software programs, when executed by the delegating device, implement the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 28, to page 6, line 12, a machine-readable storage medium (e.g., memory 202 in FIG. 2) contains one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device (e.g., 102D in FIG. 1) to at least one recipient device (e.g., 102R in FIG. 1), wherein the cryptographic functionality is characterized as a graph comprising a plurality of nodes. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page 6, lines 19-21, the one or more software programs, when executed by the delegating device, implement the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

As described in the specification at, for example, page 3, lines 10-15; page 15, lines 16-25; page 17, lines 21-26; and page 25, lines 1-28, illustrative embodiments of the present invention provide a number of advantages relative to conventional techniques. For example, an illustrative embodiment may permit delegation on a per-computation rather than per-interval basis, and thus do not require a third party to know the particular intervals or segments into which computational ability has been partitioned, nor do they require a separate transmission for each interval. Another important advantage is that an illustrative embodiment may provide a particularly efficient mechanism for the provision of cryptographic functionality in accordance with a subscription model.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-30 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0094088 (hereinafter "Okaue").

ARGUMENT

Rejection of claims 1-30 under §102(b) over Okaue

Claims 1-5, 7, 8, 17-30

With regard to the §102 rejection of claims 1-30, Appellants initially note that the Federal Circuit has recently reiterated that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. §102." *Net MoneyIN Inc. v. VeriSign Inc.*, 545 F.3d 1359, 1369, 88 USPQ2d 1751, 1760 (Fed. Cir. 2008)

The Examiner argues that the Okaue reference teaches each and every one of the limitations of claim 1. Appellants respectfully disagree.

Appellants initially note that claim 1 is directed to a method of partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. Appellants respectfully submit that Okaue discloses neither partitioning of cryptographic functionality into a plurality of distinct portions nor delegation of at least one of such distinct portions from a delegating device to at least one recipient device. As discussed in paragraph 91, the "hierarchical key tree construction . . . ensures the system to safely enable to [sic] distribute to the properly licensed devices such ciphering keys for ciphering the above-cited contents data." Ensuring distribution of keys to properly licensed devices is not analogous to delegation of a distinct portion of cryptographic functionality from a delegating device to a recipient device if the manner recited in claim 1.

Claim 1 includes limitations wherein the nodes correspond to respective seeds, wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and wherein the transmitted information includes the first seed but not the second seed.

The Examiner apparently argues that the keys associated with various nodes in Okaue are analogous to the seeds recited in claim 1. Leaving aside the issue of whether these keys would be considered seeds by one skilled in the art, however, claim 1 specifies that a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level.

There is no teaching or suggestion of any arrangement in Okaue wherein the key associated with a node at a lower level is computed as a function of a key associated with a node of a higher level. The portions of Okaue cited by the Examiner, such as paragraphs 23-24, 97-105 and 114-117, are directed to enciphering and deciphering of keys which have already been computed, rather than to computing the keys. See, for example, Okaue at paragraphs 16 and 24 (both stating that the "enabling key block (EKB) also includes such data of upper-rank keys enciphered via lower-rank keys as well") and paragraph 98 ("The Enc(Ka, Kb) designates such a data consisting of Kb which is enciphered by Ka.").

Paragraph 102 of Okaue merely indicates that a key associated with a node of a higher level may be encrypted using a key associated with a node of a lower level such that the encrypted key associated with the higher level may be decrypted using the key associated with the lower level:

> By applying the leaf key of its own, the device 2 is enabled to decode the ciphered key whereby acquiring the updated node key K(t) 001. Further, using the updated node key K(t) 001, the device 2 is also able to decode the ciphering key Enc (K(t) 001 and K(t) 00) corresponding to the second lowest rank shown in A of FIG. 4, whereby acquiring the updated node key K(t) 00. In this way, the device 2 serially decodes the ciphering key Enc (K(t) 00 and K(t) 0) corresponding to the second uppermost rank shown in A of FIG. 4, and then also decodes the updated node key K(t) 0 and the ciphered key Enc (K(t) 0 and K(t) R) corresponding to the uppermost rank shown in A of FIG. 4, whereby acquiring the updated node key K(t) R.

Such teachings fail to address the manner in which the key itself is computed, however. Indeed, the keys in Okaue are not computed as functions of one another, but rather appear to each be computed as a function of the respective leaf IDs. See paragraph 664. Thus, Okaue fails to teach or suggest the limitation of claim 1 wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level.

Moreover, claim 1 specifies that the transmitted information includes the first seed (associated with a node of the first, lower level) but not the second seed (associated with a node of the second, higher level). By contrast, Okaue clearly discloses an arrangement in which the transmitted information includes keys associated with nodes of higher levels. For example, in FIG. 4, each of the EKBs shown includes both the key associated with node 001 and the key associated with node 0010. See Okaue at paragraph 94 ("In the tree structure shown in FIG. 3, for example, the device 0 is provided with a leaf key K0000 and node keys K000, K00, K0, and KR. The device 5 is provided with a key K0101, K010, K01, K0, and KR. The device 15 is provided with a key K1111, K111, K11, K1, and KR.") See also Okaue at paragraphs 99, 102, 103 and 110-117, the latter with reference to FIG. 6.

As such, it is clear that Okaue fails to meet the limitation of claim 1 wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and wherein the transmitted information includes the first seed but not the second seed.

Accordingly, it is believed that Okaue fails to meet the limitations of independent claim 1.

Claims 2-5, 7, 8, 17-21 and 24-27 are believed allowable at least by virtue of their dependency from independent claim 1.

Independent claims 28-30 are believed allowable for reasons similar to those outlined above with regard to claim 1.

Claim 6

In addition to being allowable by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 6 is believed to define additional separately-patentable subject matter. More particularly, dependent claim 6 includes a limitation wherein the graph comprises at least first and second root nodes. The Examiner argues that this limitation is shown in Okaue at paragraphs 132 and 134. See the Office Action at page 5, third paragraph. Appellants respectfully disagree, noting that paragraph 132 of Okaue describes "a variety of systems for providing the hierarchical key tree structure shown in FIG. 3 with those ciphering keys including root keys." In other words, different systems (i.e., different structures) could include different root keys. However, Okaue does not teach or suggest any arrangement in which one graph includes at least first and second root nodes. Rather, in each of the structures shown in Okaue, there is one and only one root node. See, for example, Okaue at paragraph 134 ("In FIG. 11, a root key Kroot 1101 is installed to the uppermost rank of the hierarchical key structure.") See generally Okaue at FIGS. 3, 7, 11-14 and 44 (each showing key structures with one and only one root node). Thus, Okaue fails to teach or suggest the limitations of claim 6.

Claim 9

In addition to being allowable by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 9 is believed to define additional separately-patentable subject matter. More particularly, dependent claim 9 includes a limitation wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node.

In formulating the rejection of claim 9, the Examiner again relies on Okaue at paragraphs 23, 24, 97-105 and 114-117. See the Office Action at page 5, last paragraph. Appellants respectfully submit that the relied-upon portions of Okaue fail to disclose any arrangement in which a graph comprises levels of nodes, wherein a level comprises a parent node and a set of seeds each derivable from the parent node. As noted above with reference to claim 1, there is simply no disclosure within Okaue of a technique in which one seed is derivable from another seed. Thus, Okaue clearly fails to disclose a technique in which a level of nodes comprises a parent node and a set of seeds each derivable from the parent node, as recited in claim 9.

Claim 10

Claim 10 is allowable by virtue of its dependency from independent claim 1 and dependent claim 9, each of which is believed to be separately patentable for the reasons discussed above. Claim 10 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 10 includes a limitation wherein an *i*th node of a *k*th one of the levels is computed as $f_k(i, v_{k+1})$, where f_k is a one-way function.

In formulating the rejection of claim 10, the Examiner again relies on Okaue at paragraphs 23, 24, 97-105 and 114-117. See the Office Action at page 6, first paragraph. As noted above with reference to claim 1, there is simply no disclosure within Okaue of a technique in which one seed is computed as a function of another seed. Thus, Okaue clearly fails to disclose a technique in which a node of one of the levels is computed as a function of a seed within another level in the particular manner recited in claim 10.

Claim 11

Claim 11 is allowable by virtue of its dependency from independent claim 1 and dependent claims 9 and 10, each of which is believed to be separately patentable for the reasons discussed above. Claim 11 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 11 includes a limitation wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

In formulating the rejection of claim 11, the Examiner again relies on Okaue at paragraphs 23, 24, 97-105 and 114-117. See the Office Action at page 6, second paragraph. Appellants respectfully submit that there is no teaching within the relied-upon portions of Okaue of any technique in which nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

Claim 12

Claim 12 is allowable by virtue of its dependency from independent claim 1 and dependent claims 9-11, each of which is believed to be separately patentable for the reasons discussed above. Claim 12 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 12 includes a limitation wherein the *i*th node of a *j*th tuple of the *k*th level is computed as $f_k(j, i, v_{k+1,j})$.

In formulating the rejection of claim 12, the Examiner again relies on Okaue at paragraphs 23, 24, 97-105 and 114-117. See the Office Action at page 6, third paragraph. As noted above with reference to claim 1, there is simply no disclosure within Okaue of a technique in which one seed is computed as a function of another seed. Thus, as noted above with reference to claim 10, Okaue clearly fails to disclose a technique in which a node of one of the levels is computed as a function of a seed within another level, as recited in claim 12.

Claim 13

In addition to being allowable by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 13 is believed to define additional separately-patentable subject matter. More particularly, claim 13 includes a limitation wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token.

In formulating the rejection of claim 13, the Examiner relies on Okaue at paragraphs 30-32, 83, 85 and 87-89. See the Office Action at page 6, fourth paragraph. The relied-upon portions of Okaue merely indicate that the techniques disclosed therein could be implemented by a general-purpose computer system. Appellants respectfully submit that there is no teaching within the cited portions of Okaue, or elsewhere within Okaue, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises a cryptographic functionality provided by a hardware-based authentication token. Indeed, there is no disclosure of a cryptographic functionality provided by a hardware-based authentication token.

Claim 14

In addition to being allowable by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 14 is believed to define additional separately-patentable subject matter. More particularly, claim 14 includes a limitation wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

In formulating the rejection of claim 14, the Examiner relies on Okaue at paragraphs 30-32, 83, 85 and 87-89. See the Office Action at page 6, fifth paragraph. The relied-upon portions of Okaue merely indicate that the techniques disclosed therein could be implemented by a general-purpose computer system.

Appellants respectfully submit that there is no teaching within the cited portions of Okaue, or elsewhere within Okaue, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token. Indeed, there is no disclosure of an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

Claim 15

Claim 15 is allowable by virtue of its dependency from independent claim 1 and dependent claim 14, each of which is believed to be separately patentable for the reasons discussed above. Claim 15 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 15 includes a limitation wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

In formulating the rejection of claim 15, the Examiner relies on Okaue at paragraphs 30-32, 83, 85 and 87-89. See the Office Action at page 7, first paragraph. The relied-upon portions of Okaue merely indicate that the techniques disclosed therein could be implemented by a general-purpose computer system. There is no disclosure of a verification operation performed collaboratively by at least first and second servers each storing one of the seeds, as recited in claim 15.

Claim 16

In addition to being allowable by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 16 is believed to define additional separately-patentable subject matter. More particularly, claim 16 includes a limitation wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

In formulating the rejection of claim 16, the Examiner relies on Okaue at paragraphs 30-32, 83, 85 and 87-89. See the Office Action at page 7, second paragraph. The relied-upon portions of Okaue merely indicate that the techniques disclosed therein could be implemented by a general-purpose computer system.

Appellants respectfully submit that there is no teaching within the cited portions of Okaue, or elsewhere within Okaue, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token. Indeed, there is no disclosure of an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

In view of the above, Appellants believe that claims 1-30 are in condition for allowance, and respectfully request reversal of the present rejection.

Respectfully submitted,

Joseph B. Ryan

Date: January 4, 2010

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, the method comprising the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

2. The method of claim 1 wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality.

3. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes.

4. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph.

5. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph.

6. The method of claim 1 wherein the graph comprises at least first and second root nodes.

7. The method of claim 1 wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality.

8. The method of claim 1 wherein the graph comprises a chain.

9. The method of claim 1 wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}$, $v_{1,2}$, . . . $v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node.

10. The method of claim 9 wherein an ith node of a kth one of the levels is computed as $f_k(i, v_{k+1})$, where f_k is a one-way function.

11. The method of claim 10 wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

12. The method of claim 11 wherein the ith node of a jth tuple of the kth level is computed as $f_k(j, i, v_{k+1,j})$.

13. The method of claim 1 wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token.

14. The method of claim 1 wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

15. The method of claim 14 wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

16. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

17. The method of claim 1 wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature.

18. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain.

19. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations.

20. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations.

21. The method of claim 1 wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys.

22. The method of claim 1 wherein the cryptographic functionality comprises an ability to compute one or more seeds.

23. The method of claim 22 wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

24. The method of claim 1 wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes.

25. The method of claim 24 wherein compliance with the specified criterion is satisfied upon receipt of a designated payment.

26. The method of claim 1 wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function.

27. The method of claim 26 wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function.

28. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

the processing device being configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes, the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

29. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality;

the processing device being operative to receive from the delegating device information representative of one or more of the nodes, the processing device being configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the received information including the first seed but not the second seed.

30. A machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, wherein the one or more software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.